CLAIMS

What is claimed is:

1. A method for monitoring intrusion activity utilizing a plurality of firewalls, comprising:

(a) establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity;

(b) collecting the information from the firewalls of the computers utilizing the network; and

(c) transmitting a response to the firewalls of the computers utilizing the network;

(d) wherein the firewalls are adapted for preventing the intrusion activity utilizing the response.

2. The method as recited in claim 1, and further comprising heuristically analyzing the information to ascertain intrusion activity.

3. The method as recited in claim 1, and further comprising generating rules for preventing the intrusion activity utilizing the firewalls.

4. The method as recited in claim 3, wherein the response includes the rules.

5. The method as recited in claim 1, wherein the information is collected by the firewalls automatically.

6. The method as recited in claim 5, wherein the information is collected by the firewalls periodically.

7. The method as recited in claim 1, wherein the information is transmitted utilizing an HTTP protocol.

8. A system for monitoring intrusion activity utilizing a plurality of firewalls, comprising:

(a) logic for establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity;

(b) logic for collecting the information from the firewalls of the computers utilizing the network; and

(c) logic for transmitting a response to the firewalls of the computers utilizing the network;

(d) wherein the firewalls are adapted for preventing the intrusion activity utilizing the response.

9. A computer program product for monitoring intrusion activity utilizing a plurality of firewalls, comprising:

(a) computer code for establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity;

(b) computer code for collecting the information from the firewalls of the computers utilizing the network; and

(c) computer code for transmitting a response to the firewalls of the computers utilizing the network;

(d) wherein the firewalls are adapted for preventing the intrusion activity utilizing the response.

10. A method for reporting intrusion activity utilizing a plurality of firewalls, comprising:

(a) establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity;

(b) collecting the information from the firewalls of the computers utilizing the network;

(c) analyzing the information to ascertain intrusion activity;

(d) identifying a source of the ascertained intrusion activity; and

(e) notifying the source of the ascertained intrusion activity.

11. The method as recited in claim 10, wherein the information is heuristically analyzed.

12. The method as recited in claim 10, wherein the identification of the source includes identifying an Internet Protocol (IP) address associated with at least one source of the intrusion activity.

13. The method as recited in claim 12, wherein the identification of the source further includes looking up an electronic-mail address based on the IP address.

14. The method as recited in claim 10, wherein the notification includes an electronic mail.

15. The method as recited in claim 10, wherein the notification includes a summary of the intrusion activity.

16. The method as recited in claim 10, and further comprising determining whether a response to the notification is received.

17. The method as recited in claim 16, wherein if it is determined that the response to the notification is not received, reporting the source of the intrusion activity to a central intrusion activity watch service.

18. The method as recited in claim 17, wherein the central intrusion activity watch service notifies the public of the source of the intrusion activity via a web interface.

19. A system for reporting intrusion activity utilizing a plurality of firewalls, comprising:

(a) logic for establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity;

(b) logic for collecting the information from the firewalls of the computers utilizing the network;

(c) logic for analyzing the information to ascertain intrusion activity;

(d) logic for identifying a source of the ascertained intrusion activity; and

(e) logic for notifying the source of the ascertained intrusion activity.

20. A computer program product for reporting intrusion activity utilizing a plurality of firewalls, comprising:

(a) computer code for establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity;

(b) computer code for collecting the information from the firewalls of the computers utilizing the network;

(c) computer code for analyzing the information to ascertain intrusion activity;

(d) computer code for identifying a source of the ascertained intrusion activity; and

(e) computer code for notifying the source of the ascertained intrusion activity.

21. A method for monitoring intrusion activity utilizing a firewall, comprising:

(a) collecting information relating to intrusion activity utilizing a firewall associated with a computer;

(b) transmitting the information from the firewall associated with the computer to a central server utilizing the network;

(c) receiving a response from the central server utilizing the network;

(d) wherein the firewall is adapted for preventing the intrusion activity utilizing the response.

22. A method for monitoring intrusion activity utilizing a plurality of firewalls, comprising:

(a) establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity;

(b) collecting the information from the firewalls of the computers utilizing the network;

(c) heuristically analyzing the information to ascertain intrusion activity;

(d) generating rules for preventing the intrusion activity utilizing the firewalls based on the heuristic analysis;

(e) transmitting the rules to the firewalls of the computers utilizing the network, wherein the firewalls are adapted for preventing the intrusion activity utilizing the rules;

(f) identifying an Internet Protocol (IP) address associated with at least one source of the intrusion activity;

(g) looking up an electronic-mail address based on the IP address;

(h) generating a summary of the information relating to the intrusion activity associated with the source;

(i) transmitting the summary to the electronic-mail address in the form of electronic-mail;

(j) determining whether a response to the electronic-mail is received; and

(k) if it is determined that the response to the electronic-mail is not received, reporting the source of the intrusion activity to a central intrusion activity watch service, wherein the central intrusion activity watch service notifies the public of the source of the intrusion activity via a web interface.